STRATEGIC COMPETITION IN CYBERSPACE: CHALLENGES AND IMPLICATIONS

Annotated Bibliography

July 10-11, 2019

Center for Global Security Research
LAWRENCE LIVERMORE NATIONAL LABORATORY

Annotated Bibliography

Strategic Competition in Cyberspace: Challenges and Implications

Center for Global Security Research
Livermore, California, July 10-11, 2019

Prepared By: Ming Chen, Nenad Georgiev, Jaclyn A. Kerr, David Liu,
Kevin Neville, Oleksandr Shykov

Key Questions:

1. The 2017 National Defense Strategy argues that, in a more competitive security environment, the United States must out-think, out-partner, and out-innovate its adversaries. How does this apply to competition in cyberspace?
2. Administration leaders have set a goal of "over-matching" capabilities and strategic dominance in the technology competition. What does this mean and require in the cyber domain and what risks does it entail?
3. The National Defense Strategy Commission faults the Department of Defense for its limited progress so far in developing operational concepts that link strategy and doctrine to capability development. Are such concepts missing in cyberspace and if so, what can be done to create them?

Panel Topics:

1. Cyber Competition and U.S. Defense Strategy
2. Cyber Competition and the Changing Strategic Environment
3. Cyber's Place in Integrated Strategic Deterrence
4. Cyber's Place in Adversary Information Confrontation Strategies
5. Managing the Risks of Cyber Competition
6. U.S. Allies as Co-Competitors
7. The Promise and Limits of Public-Private Cyber Partnerships
8. Back to the Key Questions – a Roundtable Discussion

Panel 1: Cyber Competition and U.S. Defense Strategy

- Looking back over the last decade or so, what have been the main milestones in defining cyber strategy and integrating it into defense strategy? Is the critique by the NDS Commission sound?
- Looking to the future, what might be the rewards and risks of tripolar competition for strategic dominance? Have we set the right goals and metrics of success?
- What are the necessary roles of cyber diplomacy in the development of international cybersecurity, Internet, and data policies in support of U.S. national security objectives?

U.S. Department of Defense. *National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

> The summary of the 2018 National Defense Strategy outlines the Department of Defense's objectives and approaches to the new strategic environment. It notes the erosion of the United States' military advantage and the rise of China and Russia as near-peer adversaries. The unclassified version of this strategy provides a broad summary of DoD's strategic approach based on three pillars: (1) building a more lethal force, (2) strengthening alliances and attracting new partners, and (3) reforming the Department for greater performance and affordability.

National Defense Strategy Commission. *Providing for the Common Defense: The Assessments and Recommendations of the National Defense Strategy Commission*, 2018. https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf.

> In this report, the National Defense Strategy Commission assesses the National Defense Strategy (NDS) and puts forth recommendations for its execution within a steadily threatening strategic landscape. The report mostly concurs with NDS recommendations for the future U.S. force posture. However, the Commission warns that, while on the right track conceptually, the NDS fails to adequately identify the resources required to fully implement the strategy. One of the areas identified by the Commission where further investment is clearly needed is cyberspace—a domain within which the U.S. has not succeeded in competing against or deterring its adversaries as effectively as it should have. The authors also urge for seriousness in answering critical questions regarding the U.S. response to the challenges posed by the rapidly changing world, which can put American interests and security at risk.

The White House. *National Cyber Strategy of the United States of America.* Washington, D.C., 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

> The Trump administration's Cyber Strategy, the first national cyber strategy since 2003, seeks to integrate cyber into all elements of national power. The strategy is comprised of four central "pillars," including: (1) protecting the American people and homeland by securing federal networks and critical infrastructure and combatting cybercrime, (2)

promoting American prosperity by nurturing the digital economy, encouraging domestic innovation, and building the cybersecurity workforce, (3) preserving peace and stability in cyberspace by fostering norms of responsible state behavior and by attributing and deterring unacceptable behavior, and (4) advancing American influence by promoting an open, interoperable, reliable, and secure global Internet. The document emphasizes the need to utilize tailored deterrence strategies with specific threats to ensure adversaries understand the consequences of particular malicious behaviors. It also calls for the use of all appropriate tools of national power to expose and counter malign influence and disinformation campaigns.

U.S. Department of Defense. *Cyber Strategy*, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

DoD's Cyber Strategy focuses on the new era of strategic great power competition. It highlights the risks posed by China's persistent exfiltration of sensitive information from U.S. public and private sector institutions and Russia's use of cyber-enabled information operations to influence public opinion and challenge democratic processes. The strategy also stresses the need to protect the open, transnational, and decentralized Internet, and the access to reliable information it supports, holding these as vital to American prosperity, liberty, and security. The strategy outlines five main objectives, including: (1) ensuring the joint force can achieve its missions in a contested cyberspace environment, (2) enhancing U.S. military advantages by strengthening the joint force through cyberspace operations, (3) defending U.S. critical infrastructure, (4) securing DoD information against malicious cyber activity, and (5) expanding DoD cyber cooperation with interagency, industry, and international partners. The strategy emphasizes the need to act consistently and persistently in the face of adversaries operating in the same way, and to "defend forward" as a more engaged and proactive way to stop malicious cyber activity at its source.

U.S. Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

In response to the new means of influence and coercion allowing U.S. adversaries to increasingly exploit cyberspace below the threshold of armed conflict, the U.S. Cyber Command Vision adopts a new approach that seeks to improve security and stability in cyberspace. This strategy aims to achieve cyberspace superiority by increasing resiliency, defending forward, and persistently contesting and countering malicious cyber actors wherever they are found. USCYBERCOM will collaborate with other combatant commands, services, departments, allies, and industry, ultimately contributing to the United States' national strategic deterrence. Despite the risk of adversaries portraying the strategy as "militarizing" the cyberspace domain, the Command Vision recognizes that the cyber domain has already been militarized by adversaries, and therefore U.S. interests should not be jeopardized by the limitations of passive defenses.

Fischerkeller, Michael P., and Richard J. Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." *Orbis* 61, no. 3 (2017): 381-93. https://www.sciencedirect.com/science/article/pii/S0030438717300431.

> Fischkeller and Harknett argue that U.S. national cybersecurity has failed to take advantage of the security opportunities that abound from the uniqueness of cyberspace. In order for the strategy to be effective, it must align with the structural features and operational characteristics of the cyber domain. They argue that, because the operational environment is one of constant contact between adversaries, deterrence is not a credible strategy in cyberspace. Instead they suggest a strategy of persistent engagement in the cyber domain. By taking such an active and constantly reactive strategy, they argue that the U.S. will be able to establish international norms and further establish itself in the cyber realm on its own terms.

Lin, Herbert and Max Smeets. "An Outcome-Based Analysis of U.S. Cyber Strategy of Persistence & Defend Forward." *Lawfare*, November 28, 2018. https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward.

> Lin and Smeets expand on the initial research from the scholarly community on the United States' persistent engagement and defend forward strategy in cyberspace by suggesting an outcome-based analysis. Such analysis takes into account the specific casual mechanisms and scenarios as to how the consequences of the strategic shift may unfold. They also stress that further research in this field, in particular case-study analyses, is needed in order to optimize power gains and reduce escalation.

Lin, Herbert. "U.S. Cyber Infiltration of the Russian Electric Grid: Implications for Deterrence." *Lawfare*, June 18, 2019. https://www.lawfareblog.com/us-cyber-infiltration-russian-electric-grid-implications-deterrence.

> Commenting on a recently published report which revealed that the United States has deployed malware inside Russia's electric power grid, Lin comes to the conclusion that that the assumption that there is only one method for carrying out a cyber mission is likely invalid. His argument is based mostly on the fact that U.S. officials did not object to reporting on the malware implants, suggesting that there must be multiple ways to carry out the mission for their infiltration. This further casts doubt on the premise that revealing an offensive cyber capability destroys its future value as an operational asset.

Panel 2: Cyber Competition and the Changing Strategic Environment

- How do Russia, China, North Korea, Iran, and other key actors operate in cyberspace and conceptualize its role in broader forms of military, economic, and political competition?
- How do they conceive the different requirements of cyberspace operations in peacetime, crisis, and war?
- How has cyber competition affected the international security environment so far? How is this likely to develop in the future in the face of new and emerging digital technologies and the proliferation of cyber capabilities?

On China:

Segal, Adam. "Chinese Cyber Diplomacy in a New Era of Uncertainty." *Hoover Institution*, June 2017. https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.

> Segal describes China's foreign policy in the cyber domain, and the specific measures its leaders have taken to achieve it. He emphasizes the importance of cyber sovereignty for China, and the differences in the definitions used by Chinese and American decisionmakers. For example, Chinese diplomats and policymakers have a broader scope of concerns and threats that they include under the "information security" umbrella. Many of the policies that China espouses in other domains apply to the cyber world as well, such as non-interference in internal affairs through the use of the Internet.

Kania, Elsa, Samm Sacks, Paul Triolo, and Graham Webster. "China's Strategic Thinking on Building Power in Cyberspace: A Top Party Journal's Timely Explanation Translated." *New America Foundation Cybersecurity Initiative*, September 2017. https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/.

> The authors lay out the foundations of China's cyber strategy; more importantly, they explain what it entails for China to become a "cyber superpower." Some of the plans target primarily the domestic audience, such as creating and managing online content, guiding online public opinion, and managing the online ecosystem. Other policies, on the other hand, are geared to protect critical information infrastructure security, and deepen participation in and influence over international Internet governance processes.

Kania, Elsa B., and John K. Costello. "The Strategic Support Force and the Future of Chinese Information Operations." *The Cyber Defense Review* 3, no.1 (2018): 105-22. https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Strategic%20Support%20Force_Kania_Costello.pdf?ver=2018-07-31-093713-580.

> The establishment of the Strategic Support Force (SSF) in December 2015 is just one part of the PLA's recent military reforms, reflective of Beijing's desire to dominate in space, cyberspace, and the electromagnetic domain. Although it could be seen as a response to the U.S. establishment of the U.S. Cyber Command (USCYBERCOM), the SSF is unique in

several key respects: China's SSF operates as a military service and lacks a nuclear component. The SSF's cyber corps operations are highly integrated and feature a comprehensive approach to information security. The authors provide an overview of SSF, including its leadership, structure, and missions. They conclude that the establishment of the SSF and other military reforms indicate the PLA's increasing interest in information operations.

Jinghua, Lya. "A Chinese Perspective on the Pentagon's Cyber Strategy: From 'Active Cyber Defense' to 'Defending Forward'." *Lawfare*, October 19, 2018. https://www.lawfareblog.com/chinese-perspective-pentagons-cyber-strategy-active-cyber-defense-defending-forward.

Jinghua argues that the United States has consistently been unjustifiably critical of China's cybersecurity measures, gradually portraying China as an increasing cyber threat in its strategy documents. The new shift toward a proactive stance in cyberspace by the United States, she argues, is likely seen by many as a response to China's cyber posture. Contrary to U.S. beliefs, however, she claims that China does not seek an arms race with the United States; rather, it builds its cyberspace capabilities to keep up with recent trends in the military-technological revolution worldwide. Instead of pursuing a more offensive posture, which can make other countries feel anxious about their own cybersecurity, Jinghua recommends that the U.S. rethink "aggression" and exercise "self-restraint" in order to improve the security environment. In response to Jinghua's critique, Robert Chesney argues that discussing the United States' defense forward approach exclusively within the context of China threatens to miss justifications for such proactive stance stemming from the malicious cyber activities of Russia, North Korea, and Iran. He posits that, regardless of the stance the United States takes, rival states have already enough incentives to increase their cyber capabilities, particularly because the cyber domain is one in which America's advantages can be circumvented.

On Russia:

Adamsky, Dmitry. "Cross-Domain Coercion: The Current Russian Art of Strategy." *Proliferation Papers,* no. 54 (2015). https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

Adamsky traces the development of contemporary Russian military strategy and approaches to coercion, from the post-Cold War period's emphasis on regional nuclear deterrence to more recent cross-domain holistic thinking about deterrence and compellence that Western observers have described as "hybrid warfare" or the "Gerasimov Doctrine." The current "New Generation Warfare" (NGW) strategic approach, which evolved as a response to a perceived Western threat to Russia, integrates efforts across nuclear, conventional, and informational domains. Contemporary Russian operational art aims to alter adversary perceptions and manipulate decision-making processes to achieve strategic gains while minimizing the need for kinetic use of force. While some of today's tools are new, Adamsky argues that

asymmetric, indirect, psychological approaches have historically played an important role in Russian, Tsarist and Soviet strategies. The article stresses conceptual distinctions in Russian-language terminology—such as the use of *sderzhivanie* (deterrence) in a defensive connotation and the use of *prinuzhdenie* (compellence) in an offensive connotation—emphasizing the importance of these concepts to understanding the Russian *modus operandi*, especially in the fields of NGW and information warfare.

U.S. Senate, Select Committee on Intelligence. *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*. 115th Cong., 1st sess., Washington, DC: Government Publishing Office, 2017. https://www.hsdl.org/?view&did=802222.

This Congressional testimony for the U.S. Senate Select Committee on Intelligence seeks to highlight the issue of Russian active measures and influence campaigns. Roy Godson, professor emeritus at Georgetown University first outlines the use of active measures as a strategic weapon that has historically been used by the Soviet Union and now Russia, in addition to evidence of Russia's current active measures, which Clint Watts argues is more successful now than ever due to the availability of social media to disseminate disinformation. The article further provides testimonies from FireEye, a well-known cybersecurity company, and from General Keith B. Alexander, who emphasizes the role of ICTs in Russia's active measures campaigns, and the necessity of public-private cooperation in combatting the issue. Thomas Rid concludes with an analysis of the 2016 active measures campaign carried out by Russia, and the role of the information environment in enabling that.

Jensen, Benjamin, Brandon Valeriano, and Ryan Maness. "Fancy Bears and Digital Trolls: Cyber Strategy With a Russian Twist." *Journal for Strategic Studies* 42, no. 2 (2019): 212-34. https://doi.org/10.1080/01402390.2018.1559152.

This article examines how Russia exploits the digital domain to achieve relative advantage over its adversaries. The authors explain that cyber operations are usually employed by Russia to delegitimize their rivals prior to conflict, to support combat operations during conflict, and to create chaos after conflict. They argue that these actions, although concerning, generally fail to coerce in a direct manner. This prompts the authors to question the efficacy of Russia's strategical actions within cyberspace.

On North Korea:

Haggard, Stephan, and Jon R. Lindsay. "North Korea and the Sony Hack: Exporting Instability Through Cyberspace." *Asia Pacific,* no. 117 (2015). https://www.eastwestcenter.org/system/tdf/private/api117.pdf?file=1%26type=node%26id=35164.

Haggard and Lindsay argue that North Korean capabilities and tactics largely reflect an already-established military doctrine. Provocations are carefully calculated so that they neither inflict too many casualties nor bring large-scale destruction. As a result, these attacks go unpunished. In other words, North Korea mastered the art of provocation and

now they apply it in the cyber domain. North Korean cyber capabilities have grown since the 1980s when with the help of the CCP, they jumpstarted their program. By some measures, North Korea now employs 1,400 cyber operators. Although many still view North Korea as desperately backward, the Kim family keeps surprising the international community with nuclear and now cyber weapons.

On Iran and the Middle East

Herr, Trey, and Laura K. Bate. "The Iranian Cyberthreat Is Real." *Foreign Policy*, July 26, 2017. http://foreignpolicy.com/2017/07/26/the-iranian-cyberthreat-is-real/.

Iran has been at the focus of the international community mostly because of its potential nuclear capabilities. However, Herr and Bate argue that Iran's cyber-enabled operations are another aspect of Iran's provocative foreign policy that should be given equivalent attention. Iran's cyber capabilities have developed and grown in sophistication. The authors argue that Iran's cyber doctrine and capabilities were influenced by its own experiences as a target of cyberattacks, most notably Stuxnet in 2012 which slowed down its nuclear enrichment program. After having one of their own oil facilities attacked by a malware designed to wipe computer systems of data, Iran responded with an equal attack against a Saudi oil producer and a Qatari gas producer, which forced the replacement of tens of thousands of computers.

Anderson, Collin and Karim Sadjadpour. *Iran's Cyber Threat: Espionage, Sabotage, and Revenge* (Washington, DC: Carnegie Endowment for International Peace, 2018). https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf.

While Iran has been a recurring target of offensive and destructive cyber operations by the United States and its allies, Anderson and Sadjadpour note that Iran has also been increasingly using cyber means to conduct espionage and retaliate against its perceived opponents both at home and abroad. Despite not having the capabilities of the United States, China, or Russia, the authors stress that Iran's modestly funded but indigenously developed cyber capabilities have sometimes extorted significant political and economic costs on the part of the U.S., Europe, Saudi Arabia, and Israel, allowing, as a consequence, Iran to project itself as an emerging cyber power. Because Iran does not have a public strategy with respect to cyberspace, a better understanding of the strategic rationale of its past cyber activities might be key in order for the United States to adapt its future posture and responses to Iran's cyber threat. To this end, the authors suggest a number of policy approaches that include: (1) utilizing existing frameworks for targeted sanctions or indictments, (2) improving information sharing on threats across communities, and (3) supporting initiatives to improve information security.

Shires, James. "Cybersecurity Governance in the GCC." In *Rewired: Cybersecurity Governance,* edited by Ryan Ellis and Vivek Mohan, 19-37. Hoboken, NJ: Wiley, 2019. https://docs.wixstatic.com/ugd/92024e_aa6b006d649b4d45b8ba047f03eb7eee.pdf?index=true

> Shires in this chapter studies cybersecurity governance in the six states of the Gulf Cooperation Council (GCC): Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates. While not a major threat, the author notes that all these states have governing characteristics that are underrepresented in the literature on cybersecurity, which has predominantly focused on Western countries and their traditional competitors, China and Russia. Shires' discussion of cybersecurity governance spans the following three themes: the regional specificity of cybersecurity governance; the importance of an international image of cybersecurity governance; and the reinterpretation of the scope of cybersecurity governance for political purposes.

Emerging Technologies, Digital Authoritarianism, and Proliferation:

Horowitz, Michael B., Gregory C. Allen, Elsa B. Kania, and Paul Scharre. "Strategic Competition in an Era of Artificial Intelligence." *Center for a New American Security*, July 2018. https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence.

> This article provides an overview of artificial intelligence (AI) technology and its potential role in a new era of strategic competition. The authors frame AI as a technology that is more akin to electricity or the combustion engine than to a specific weapon. The article provides country case studies of AI capability development in China, Russia, and India, considering these states' efforts at national planning, public-private cooperation, and military incorporation of AI. The authors conclude that if the United States hopes to remain competitive in AI development, it needs to create an effective, comprehensive strategy to develop and implement AI.

Wright, Nicholas, ed. "AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives." A Strategic Multilayer Assessment (SMA) Periodic Publication, December 2018. https://nsiteam.com/ai-china-russia-and-the-global-order-technological-political-global-and-creative-perspectives/.

> This collection of 26 essays addresses the role of AI, big data, and the Internet in reshaping global politics in the 21st century—both through transforming the nature of domestic politics and political regime types, and through altering the dynamics of international conflict and global power contestation. Contributors examine the variety of emerging models of digital authoritarianism and digital liberal democracy, examining differences, for example, between the Russian and Chinese approaches to the use and control of digital information technologies at home and abroad, and the diffusion of these differing models to states around the world. The authors conclude with a series of recommendations to U.S. policymakers for preserving liberal democracy and global stability.

Kerr, Jaclyn. "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region." *International Journal of Communication*, 12 (2018): 3814-34. https://ijoc.org/index.php/ijoc/article/view/8542/2460.

> This article examines the complex interdependencies that exist today between national systems of digital control in different nondemocratic countries. It compares Internet policies across the former Soviet region, showing that many of the nondemocratic countries in this region have adopted similar approaches to control Internet content and use within their territories. With close examination of specific control practices tracing the roles of diffusion and coordination mechanisms, the article demonstrates how, even as overall Internet repression levels have increased, the particular legal frameworks, technical systems, and other control practices used have been deeply influenced by complex regional interdependencies. The article is part of a special issue examining the global development of digital authoritarian practices.

Panel 3: Cyber's Place in Integrated Strategic Deterrence

- What role does the cyber domain play in integrated strategic deterrence, following the reassignment of the mission from STRATCOM to CYBERCOM? What role can and should it play?
- What are the respective roles of deterrence, persistent engagement, and norms-based strategies in the cyber domain at different levels of conflict? Where is there disagreement about risks and merits of approaches?
- What more thinking about cyber strategy should be done? By whom?

Nye Jr., Joseph S. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (2017): 44-71.
https://www.belfercenter.org/sites/default/files/files/publication/isec_a_00266.pdf

> Nye seeks to clarify the conceptual and policy implications of applying deterrence theory in cyberspace. He argues that the ambiguous nature of cyber threats and their status under international law, the variety of actors, and the challenges of attribution reduce the role that deterrence by punishment can play in cyber strategy, necessitating a different approach to deterrence and dissuasion. He identifies four main mechanisms to reduce and prevent adverse actions, including (1) threat of punishment, but also (2) denial through defense and resilience, (3) entanglement, and (4) the establishment of norms and taboos. Though these approaches go beyond common conceptions of deterrence strategy based on nuclear deterrence models, he suggests that each imposes costs to prevent malicious adversary activities in cyberspace. While deterrence by punishment—including intra-domain retaliation—will likely still play a role at some levels of escalation, Nye emphasizes the benefits of approaches that might carry lower risks of escalation or can influence behavior even in the absence of immediate attribution.

Fischerkeller, Michael, and Richard Harknett. "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation." *Institute for Defense Analysis*, 2018. https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx

> Escalation dynamics resulting from any proactive posture in cyberspace taken by the United States are mainly discussed in the scholarship in terms of the potential for episodic conflict to result in physical damage or loss of life. Fischerkeller and Harknett argue that such focus is narrow and limited as it fails to distinguish between escalation and competitive interaction. The latter, the authors argue, is the predominant cyberspace dynamic, involving ongoing, long-term "agreed competition," characterized by operations that generate effects short of armed conflict equivalence. The authors posit that the persistent engagement strategy allows for operational designs that can limit escalation whether by using precise targeting as signaling while reducing collateral damage and public awareness, or by careful management of operational effects, allowing, for example, for reversible damage. If pursued strategically by the United States, the article suggests, these approaches can lead not only to operational de-escalation, but can also gradually clarify the rules (e.g., behavioral norms) of the ongoing competitive engagement and lead to increased stability.

Healey, Jason. "The Implications of Persistent (and Permanent) Engagement in Cyberspace." *Journal of Cybersecurity* (forthcoming).

> This theory-building article examines the potential relationships between "persistent engagement strategy" and stability in cyberspace. The article interrogates the prediction of the strategy's proponents that an assertive "defend forward" posture will, over time, be stabilizing, leading to tacit bargaining through repeated engagements and the emergence of agreed upon expectations concerning acceptable and unacceptable behavior. In order to better understand the underlying dynamics and their potential contributions to escalation or stability, Healey argues that we must consider alternative possible positive (escalatory) and negative (de-escalatory/stabilizing) feedback loops that might develop as a result of behavioral interactions between adversaries, either amplifying or inhibiting cyber conflict. While pointing to some mechanisms by which the strategy could indeed be stabilizing, he also indicates a number of more escalatory possibilities whereby the more assertive approach could lead to unintended consequences. One risk, for example, is that declaring a posture of "offense in the best defense" prompts more adversaries to do likewise, leading more states to develop and use offensive capabilities. The article concludes by offering several policy suggestions while also arguing for additional research to understand the actual dynamics and interactions that result from persistent engagement in different contexts and between various sets of actors.

Lindsay, Jon, and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in *The Power to Hurt: Coercion in Theory and in Practice*, edited by Kelly M. Greenhill and Peter J.P. Krause, 179-204. New York, NY: Oxford University Press, 2018. https://pdfs.semanticscholar.org/78b8/e7abf96e4ab276dc05a91beab4055fba9836.pdf.

> Lindsay and Gartzke discuss the conceptual evolution of cross-domain deterrence (CCD) which emerged as a concept in the late 2000s and has influenced many American policymakers as well as their counterparts in foreign countries. The cyber domain is unlike others in the sense that it is not physical per se like land, air, and space. Yet cyber is not a "separate territorial space" since all the communications satellites, submarine cables, servers etc. are based somewhere. It occupies a dominant place in cross-domain deterrence. The director of the U.S. Air Force in 2006 declared that "Cyber is the United States' Center of Gravity—the hub of all power and movement, upon which everything else depends. It is the nation's neural network." The authors also point out that classical deterrence was agnostic about the means of deterring the adversary as it was assumed that nuclear weapons did the trick. CCD pays more attention to the means of deterrence emphasizing the interconnections between domains. Overall, the authors perceive that the myth of the offensive cyber advantage is overblown, as there are a number of reasons an adversary is limited in its cyber-attack vectors.

Gartzke, Erik, and Jon R. Lindsay. "Thermonuclear Cyberwar." *Journal of Cybersecurity* 3, no.1 (2017): 37-48. https://doi.org/10.1093/cybsec/tyw017.

> According to Gartzke and Lindsay, the warfighting advantages of offensive cyber operations, when combined with nuclear weapons, become dangerous liabilities for nuclear deterrence. The authors argue that during a brinkmanship crisis, the risk of miscalculation is raised by the increased uncertainty about the nuclear/cyber balance of power. Cyber operations, especially those against nuclear control, command, and communications, must be conducted in secrecy in order for the attack to be successful. Because cyber operations are generally ill-suited for signaling, to reduce the risk of crisis miscalculation, the authors propose that states should improve rather than degrade mutual understanding of their nuclear deterrents.

Schneider, Jacquelyn. "Deterrence in and Through Cyberspace," in *Cross-Domain Deterrence: Strategy in an Era of Complexity,* edited by Erik Gartzke and Jon R. Lindsay, 95-121. New York: Oxford University Press, 2018. https://www.academia.edu/30652154/Cyber_and_Cross_Domain_Deterrence_Deterring_Within_and_From_Cyberspace.

> Drawing from existing literature on cyberspace operations and deterrence, Schneider explores the role of cyber operations in cross-domain deterrence and deterrence of cyber operations within cyberspace. By looking into the major limitations and concerns for cyberspace deterrence, the author focuses on the challenges and opportunities that uncertainty pose for U.S. cyber deterrence policies. She argues that while the United States could embrace and leverage uncertainty for its strategic benefit, there are several steps that can be taken if uncertainty is unacceptable for the United States. Some of

these steps include investing in attribution technologies, focusing on tailored high-threshold deterrence, advocating declaratory punishment policies, and advocating behavioral norms in cyberspace.

Kreps, Sarah E., and Jacquelyn Schneider. “Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics.” SSRN, 2018. http://dx.doi.org/10.2139/ssrn.3104014.

In order to examine whether nuclear strategist Herman Kahn’s effects-based ladder of escalation is relevant in the information age, the authors conducted an empirical study followed by a survey which involved questions regarding retaliatory measures in the three domains: cyber, conventional, and nuclear. Based on their findings, the authors concluded that there is a clear firebreak between the three domains. American support for retaliation for cyberattacks cannot be explained solely by the effects created by attacks, because they see cyberattacks as qualitatively different than those of similar magnitude from other domains. Such findings cast doubt on the logic of cyber deterrence that rests on the United States having the political resolve to retaliate for a cyberattack.

Miller, James N., and Neal A. Pollard. “Persistent Engagement, Agreed Competition and Deterrence in Cyberspace.” *Lawfare*, April 30, 2019. https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace.

In relation to the strategy of persistent engagement, Miller and Pollard discuss the notion of “agreed competition.” They argue that, in the attempt to define the boundaries of agreed competition, it is of utmost importance not to inadvertently suggest to allies or adversaries that hostile acts such as North Korea’s Sony Entertainment hack, Iran’s DDoS attack on Wall Street, China’s cyber-enabled theft of intellectual property, or Russia’s cyber-enabled disinformation campaigns fall within the notion of “agreed competition.” To do so would undermine any prospect of establishing effective deterrence of such offensive actions. The authors posit that rather than assuming that a cyberspace-only agreed competition exists or will exist, it should be recognized that there are multiple simultaneous agreed competitions in the economic, diplomatic, informational and military spheres, each of which involves cyberspace. Agreed competition with respect to the persistent engagement strategy has been a topic of ongoing recent debate in Lawfare, including contributions from Jacquelyn G. Schneider, Max Smeets, and Richard Harknett and Michael Fisherkeller.

Slayton, Rebecca. "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41, no. 3 (2017): 72-109. https://cornell.app.box.com/s/58xm5d4xwbdjq549vx5xnwc3qu1dqybk.

Much of the discourse regarding cyber conflicts conclude that the offense has an inherent technological advantage. Slayton argues that such claims are deeply misguided, and she provides a framework with which to understand the causes of offensive and

defensive advantage, and to measure the utility of offensive and defensive strategies. She finds that offensive cyber operations have been more successful due to decisionmakers' valuation of certain types of attack, the organizational competence of technology management, and differences in goals. Slayton concludes that cyber defensive success is limited not by technological disadvantages, and that a defensive advantage is possible with sustained commitments to technology management, innovation and skill.

MeriTalk. "Cyberspace Solarium Commission Gets to Work". May 9, 2019. https://www.meritalk.com/articles/cyberspace-solarium-commission-gets-to-work/.

As part of the 2019 National Defense Authorization Act, the Cyberspace Solarium Commission was established with the aim to "build a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences as the world enters a new phase of cyberconflict." To this end, by bringing together members from national intelligence, homeland security, defense, as well as representatives selected by the House and Senate, the commission is charged with addressing a number of topics, such as the pros and cons of strategic frameworks, adversaries' strategies and intentions, resource allocation needs, and potential revision of government structures or authorities.

Panel 4: Cyber's Place in Adversary Information Confrontation Strategies

- What are those strategies? How do their means and ends differ from cold war propaganda strategies?
- Among the tools of information confrontation, what is the relative importance of cyber?
- What implications follow from the asymmetric vulnerabilities of democratic and non-democratic states to such strategies?

Lin, Herbert and Jaclyn Kerr. "On Cyber - Enabled Information/Influence Warfare and Manipulation." In *Oxford Handbook of Cyber Security*, edited by Paul Cornish. Oxford, UK: Oxford University Press (forthcoming). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680.

Lin and Kerr examine the recent emergence of new forms of "cyber-enabled information/influence warfare and manipulation" (IIWAM) campaigns, that are distinct both from conventional understandings of cyber domain conflict and from prior forms of information warfare or active measures. While sharing characteristics with predecessor forms of information and psychological operations, these new campaigns rely heavily on new digital information technologies, combining scalable content reproduction and targeting with cyber tools such as hacking and digital espionage. Conceptualizing this new form of conflict, the article provides an overview of the role of cyber-enabled IIWAM campaigns in the contemporary information environment, including an assessment of the psychological basis for these types of attacks. The article notes various examples of cyber-enables IIWAM campaigns involving both adversarial states and non-state groups and includes a case study of the role of such operations in recent Russian strategy. The authors suggest that democracies are especially vulnerable to IIWAM campaigns, and

that states like Russia have already taken advantage of liberal democracies' susceptibility to this type of attack. For this reason, it is critical that a coherent state response be developed, allowing for the rapid identification of IIWAM attacks and providing steps to counter its effects.

Powers, Shawn, and Markos Kounalakis, eds. *Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation*. Advisory Commission on Public Diplomacy, U.S. Department of State, 2017. https://www.state.gov/wp-content/uploads/2019/05/2017-ACPD-Internet.pdf.

The compilation of 14 essays provides an overview of public diplomacy's role in the contemporary information environment. Most contributors reject the idea of "post-truth" narrative, arguing that truth and facts matter to citizens and to the public discourse. Defining "computational propaganda" as the coordinated use of social media platforms, autonomous agendas and big data directed towards the manipulation of public opinion, the authors voice concern about the proliferation of AI-empowered bots and their usage by adversarial state actors. The contributors stress the ongoing importance of "strategic narratives" to the future of public diplomacy.

Woolley, Samuel C., and Philip N. Howard. "Computational propaganda worldwide: Executive summary." working paper, 2017. http://275rzy1ul4252pt1hv2dqyuf.wpengine.netdna-cdn.com/wp- content/uploads/2017/07/Casestudies-ExecutiveSummary-1.pdf.

This Oxford Internet Institute study analyzes numerous case studies of computational propaganda in order to better understand its global scope. This large-scale project featured the work of 12 researchers across nine countries, in total reviewing tens of millions of posts on seven different social media platforms. The case studies incorporated several different social and data science methods, including qualitative and quantitative analyses, and big data analysis of users on Facebook, Twitter, Weibo and WhatsApp. The study elucidates useful information about the trends and behavior of bots in various contexts, including valuable cross-national comparisons to support policies regarding computational propaganda issues.

Wanless, Alicia, and Berk, Michael. "Participatory Propaganda: The Engagement of Audiences in the Spread of Persuasive Communications." Social Media & Social Order Conference Proceedings. Oslo, Norway, December 2017. https://lageneralista.com/wp-content/uploads/2018/03/A-Participatory-Propaganda-Model-.pdf.

The authors offer a new model for understanding propaganda and its effects in the digital age which they call "participatory propaganda." Defined as "deliberate, systematic attempt to shape perceptions, manipulate cognitions and direct behavior of a target audience while seeking to co-opt its members to actively engage in the spread of persuasive communications, to achieve a response that furthers the desired intent of the propagandist." In the past, the objective of propaganda was to sway one's opinion in a certain direction. With the dawn of social media, the objective of propaganda expanded to include making subject also the new 'originator.' Wanless and Berk explain how

participatory propaganda operates and lay out the ingredients (e.g., hyper-targeted audience analysis, provocative content, echo chambers, manipulating feed & search algorithms, encouraging followers to action, and use of traditional media). The article is particularly timely and relevant for liberal democracies, and warns about long-term effects of participatory propaganda and the erosion of facts-based political discourse.

Giles, Keir. *Handbook of Russian Information Warfare*. Rome, Italy: NATO Defence College, 2016. http://www.ndc.nato.int/news/news.php?icode=995.

This publication presents an introductory guide to Russia's concept of information warfare, including elements of cyber warfare. The handbook specifically covers: (1) essential concepts and terminology used in Russian information warfare; (2) aims and objectives of Russian information warfare; (3) historical development and current techniques; and (4) the challenges these may pose for NATO in the future. The handbook intends to familiarize the reader with how Russia combines effort of cyber offensive operations with traditional subversion and active measures to project state power—the implications of which could be critically important for all alliance members.

Polyakova Alina. "Weapons of the weak: Russia and AI-driven asymmetric warfare." Brookings Institution, November 15, 2018. https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.

Polyakova looks into how Russia could leverage artificial intelligence advances to further its cyberattacks, disinformation campaigns, and political influence—tools that have been central to Russia's strategy to project power both toward the West and its immediate neighborhood. Polyakova argues that Russia's innovation in its information operations has not been based on technical advances, but rather on innovative utilization of ready-made commercial tools and digital platforms that offer the opportunity to be weaponized in a cost-effective manner. Because advances in deep learning, affective computing, and natural language processing makes it easier to extract sensitive information critical for manipulating human emotions, the author considers that AI would therefore provide Russia with additional comparative advantage against its adversaries. To respond to such AI-driven asymmetric warfare, Polyakova puts forth several suggestions for designing a deterrence strategy.

Lim, Gabrielle, Etienne Maynier, John Scott-Railton, Alberto Fittarelli, Ned Moran, and Ron Deibert. "Burned After Reading: Endless Mayfly's Ephemeral Disinformation Campaign." Citizen Lab, May 14, 2019 https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign/.

This report by University of Toronto's Citizen Lab reveals a vast disinformation campaign in the Middle East which has operated since 2016 through the use of fake social media accounts and imitations of legitimate news organizations and think tanks. The authors have dubbed the overarching campaign *Endless Mayfly* and argue that Iran has been its chief supporter since its operations began. Through an array of tactics such as liaising with reputable journalists and activists and publishing fraudulent articles and

reports, *Endless Mayfly's* chief objective has been to drive geopolitical discord, most prominently aiming to influence U.S. relations with Saudi Arabia and Israel. While certain metrics such as retweets, comments, and likes can indicate how much coverage such false information received, it is still unclear to what degree the campaign's operations have swayed public opinion.

Shires, James. "Hack-and-Leak Operations: Intrusion and Influence in the Gulf." Journal of Cyber Policy (forthcoming).

> This article argues for conceptualizing hack-and-leak operations (HLO) as a distinct category of cyber operation, through a close analysis of a crucial HLO that has been bypassed by the cybersecurity literature: the release of documents from the Saudi Ministry of Foreign Affairs by the "Yemen Cyber Army." It proposes a tripartite framework for understanding the impact of HLO as mechanisms of delegitimization, based on their technical characteristics, social and political context, and target audiences. The article suggests that the Yemen Cyber Army incident could have been an experiment for the same Russian actors who carried out the 2016 DNC operation, allowing them to hone their tactics prior to the U.S. elections.

Starbird, Kate. "Examining the Alternative Media Ecosystem Through the Production of Alternative Narratives of Mass Shooting Events on Twitter." *ICWSM* (2017): 230-39. https://faculty.washington.edu/kstarbi/Alt_Narratives_ICWSM17-CameraReady.pdf.

> Starbird examines the alternative media ecosystem through a qualitative analysis of mass shooting events and associated conspiracy theories using data collected from the Twitter Streaming API, which was then mapped into a domain network. The analysis accounted for several factors including account type, narrative stance coding, primary orientation, and political leaning, and also feature the interconnectivity of nodes between different alternative narrative sites. The study found evidence of alternative narratives serving underlying political agendas. The commonly-held notions of agendas of U.S. alt-right and U.S. alt-left did not apply; rather, all the selected tweets featured anti-globalist themes. In addition, content supporting Russian government interests were present in many of the selected domains. Starbird's findings provide much-needed insight into the structure of alternative narrative production, and illuminate how users engaging in alternative narrative discourse cite different web domains.

Panel 5: Managing the Risks of Cyber Competition

- What role, if any, can formal legal measures, negotiated among competitors, play in managing risks?
- What role can informal mechanisms play, including but not limited to norm creation?
- What impact are the law of war and the just war tradition likely to have in restraining cyber war and cyber competition? What about economic and social interdependencies?
- What unique risks and governance challenges are posed by conflict and competition in cyberspace? Are there relevant roles for non-state stakeholders, international institutions, or alternative governance models?

Nye Jr., Joseph S. "The Regime Complex for Managing Global Cyber Activities." *Global Commission on Internet Governance*, no. 1 (2014). https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

> Nye posits that "while there is no single regime for the governance of cyberspace, there is a set of loosely coupled norms and institutions that ranks somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and intuitions with no identifiable core and non-existent linkages." This "regime complex" includes interdependent issues, some of which relate closely to state interests, and others of which are more transnational and require collaboration across a variety of stakeholders. Nye suggests that trying to develop an all-encompassing treaty might be counterproductive, and that states should instead focus on coming to agreements limited to certain areas of concern.

Hinck, Garrett. "Private Sector Initiatives for Cyber Norms: A Summary." *Lawfare*, June 25, 2018. https://www.lawfareblog.com/private-sector-cyber-norm-initiatives-summary.

> The UN's 2016-2017 Governmental Group of Experts' (GGE) failure to come to agreement on the correct application of international law in cyberspace leaves three possible paths forward for continued discussion—through the UN, tailored norms for specific issues, or a private sector-led agreement. Hinck argues that the private sector has a significant role to play in this, and focuses on Microsoft's "Digital Geneva Convention," which proposes a three-part plan for governments to implement international rules to protect civilian use of the internet, and already had 34 signatories in June of 2018. As international governmental efforts continue to struggle to come to a consensus, initiatives from the private sector may continue to play an increasingly important role. For more on Microsoft's recent efforts to build norms and digital peace, see their Digital Peace blog.

Lin, Herbert. "Governance of Information Technology and Cyber Weapons." In *Governance of Dual-Use Technologies: Theory and Practice,* edited by Elisa D. Harris, 112-158. Cambridge, MA: American Academy of Arts & Sciences, 2016. https://www.amacad.org/sites/default/files/academy/multimedia/pdfs/publications/researchpapersmonographs/GNF_Dual-Use-Technology.pdf.

> Lin provides insight into the international effort to govern information technology and cyber weapons. Ultimately, he argues that there are four reasons that explain why governance measures for cyber weapons have not been widely adopted, including (1) the ease of creating cyber weapons; (2) their utility for governments; (3) that cyber weapons often do not cross dangerous thresholds; and (4) that so many paths lead toward cyber capability proliferation that it would be difficult for governments to effectively govern. The author concludes that the prospects for effective international governance of cyber weapons are grim, with too many stakeholders standing to gain from the use of cyber weapons.

Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York, NY: Cambridge University Press, 2013. http://csef.ru/media/articles/3990/3990.pdf.

> In 2009, the NATO Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia, invited the International Group of Experts (IGE), a group of independent experts on law and armed conflict, to produce a manual designed to provide "some degree of clarity to the complex legal issues surrounding cyber operations." The article focuses on two bodies of international law. The first, *jus ad bellum*, governs use of force as it relates to states' entry into war and includes issues related to national sovereignty, responsibility, the prohibition of the use of force, self-defense, and just war. The second body, *jus in bello*, addresses the rules of armed conflict once war has begun, including issues like discrimination of permissible targets, proportionality, occupation, and neutrality. The Tallinn Manual makes an effort to address the global understanding about the boundaries of acceptable and unacceptable actions in cyberspace.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. New York, NY: Cambridge University Press, 2017.

> The Tallinn Manual 2.0 teaches us about how the cyber threat landscape has evolved in the time since the first Tallinn manual. The change of the title from addressing "cyber warfare" to "cyber operations" indicates the shift in focus of the updated manual from conventional state-authorized and operated cyber warfare, to smaller scale deniable cyber activities that characterize cyberspace today. While the original Tallinn manual focused on the most severe cyber operations, such as those that violate the prohibition of the use of force in international relations, the new version focuses on a legal analysis of the cyber incidents that are common today, those which fall beneath the thresholds of the use of force in armed conflict. The second Tallinn Manual presents a myriad of legal questions that have arisen from cyber operations, and discusses how international law might be applied in specific scenarios, illustrating the legality of current cyber operations.

Hampson, Fen Osler, and Michael Sulmeyer, eds. *Getting Beyond Norms: New Approaches to International Cyber Security Challenges*. Waterloo, Canada: Center for International Governance Innovation, 2017. https://www.cigionline.org/sites/default/files/documents/Getting%20Beyond%20Norms.pdf.

> This collection of essays discusses potential solutions to the risks posed in cyberspace both by rapidly shifting geopolitical competition and by the increased interconnectedness and reliance of critical infrastructure sectors and services on the Internet of Things. Each of the essays examines the role of internationally agreed norms for addressing specific cybersecurity concerns and looks into whether the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security remains the appropriate venue for such discussions. All conclude that international agreement can be reached, but there needs to be a shift of thinking surrounding cybersecurity issues, whether at the intergovernmental, state, or public level.

French Ministry of Foreign Affairs. *Paris Call for Trust and Security in Cyberspace.* 2018. https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf.

> This is an initiative by the French Ministry of Foreign Affairs that calls for establishing international norms for the internet, including good cyber hygiene and coordinated disclosure of technical vulnerabilities. There are nine goals outlined in this document, some of which include developing ways to prevent the proliferation of malicious ICT tools, taking steps to prevent non-state actors from retaliating for a hack or a cybercrime, and helping to ensure foreign actors do not interfere with elections, among the rest. As a response to this document, which was endorsed by a majority of private sector and all 28 EU Member States, a multi-stakeholder debate has also been organized to discuss the role of global cyber norms, and the need for an independent body to oversee the level of security in cyberspace.

Panel 6: U.S. Allies as Co-Competitors

- What can allies contribute to cyber competition? How can they help to out-think and out-innovate cyber competitors?
- How has NATO approached the cyber challenge? How have U.S. allies and partners in Asia?
- What particular equities of theirs should the United State government understand?

Shea, Jamie. "NATO: Stepping up its Game in Cyber Defence." *Cyber Security* 1, no. 2 (2017): 165-74. https://www.henrystewartpublications.com/sites/default/files/CSJ1_2_Shea.pdf.

> Shea, the NATO Deputy Assistant Security General for Emerging Security Challenges, seeks to outline the steps that NATO has taken to address the cyber threat posed to its allies. NATO's Warsaw Summit in July 2016 set two major initiatives, including the designation of cyber as the fifth domain of warfare (in addition to land, sea, air, and space), and the Cyber Defense Pledge. In addition to these statements, NATO has sought to bolster cooperation between member states through the Cyber Defense Committee, and has made efforts to extend cyber cooperation and assistance to partner states outside of NATO as well. These moves signify NATO's moves towards making cyber defense a part of its core collective defense mission.

Hammock, C. J. "Enabling the Development and Deployment of NATO Cyber Operations: An Analysis of Modern Cyber Warfare Operations and Thresholds of Global Conflict." *Journal of Information Warfare* 16, no. 3 (2017): 79-94. https://www.researchgate.net/publication/319089829_Enabling_the_Development_and_Deployment_of_NATO_Cyber_Operations_An_Analysis_of_Modern_Cyber_Warfare_Operations_and_Thresholds_of_Global_Conflict.

Hammock focuses on NATO's cyberspace practices following the Alliance's declaration of cyberspace as a domain. The article likens the correlative behaviors between the Cold War submarine naval operations to modern cyberspace operations utilized by NATO. The article identifies challenges regarding the predictability of computer network exploitations launched by adversaries, and also highlights difficulties in attribution, countermeasures, and triggers of conflict as NATO seeks to address the threats posed to its member states in cyberspace.

Arts, Sophie. "Offense as the New Defense: A New Life for NATO's Cyber Policy." *German Marshall Fund of the United States*, December 13, 2018. http://www.gmfus.org/publications/offense-new-defense-new-life-natos-cyber-policy.

Arts argues that NATO has not yet taken the appropriate steps to prepare a comprehensive strategy in light of the rapidly evolving cyber threat landscape. While individual alliance members, like the United States, could take upon the role to fill any gaps in strategy, Arts posits that without a well-defined cyber approach at alliance level could lead to unintended consequences that might potentially escalate to conventional conflict. By formalizing its cyber strategy, NATO could establish clear thresholds for cyberattacks and define proportional response scenarios—steps that might be crucial for mobilizing member states to invoke Article 5 in a cyber crisis.

Kallender, Paul, and Christopher W. Hughes. "Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace." *Journal of Strategic Studies* 40, no. 1-2 (2017): 118-45. https://warwick.ac.uk/fac/soc/pais/people/hughes/researchandpublications/articles/hughes_and_kallender_jjs_2017_japans_emerging_trajectory_as_a_cyber_power.pdf.

Kallender and Hughes argue that Japan has become a cyber power, and built a consensus in which cybersecurity occupies the center of its national security policy. In fact, Japanese efforts in cyberspace correspond and reflect a broader transformation of its security posture both the regional and global levels. Japan's stance has moved toward the securitization and now increasing militarization of responses to challenges in the cyber domain. These efforts produced better integration of Japanese capabilities and strategy with those of the United States to better address threats from China and North Korea.

Smeets, Max. "Cyber Command's Strategy Risks Friction with Allies." *Lawfare*, May 28, 2019. https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies.

This article adds to the debate on the consequences of implementing the U.S. Cyber Command's strategy of persistent engagement, which has thus far been mostly focused on the risks of escalation. Rather than assessing how the USCYBERCOM's strategy could change the dynamics between the United States and its adversaries, Smeets looks into how the strategy might affect broader alliance relationships, especially beyond the U.S., Australia, Canada, the United Kingdom, and New Zealand. The author argues that USCYBERCOM's mission to cause friction in adversaries' freedom of maneuver in

cyberspace may end up causing significant friction in allies' trust and confidence—something which adversaries may be able to exploit in their favor.

Panel 7: The Promise and Limits of Public-Private Cyber Partnerships

- How is cyber competition for national security changing civilian cyberspace and technology sector development?
- What can the private sector do to help out-think and out-innovate cyber competitors?
- What additional equities constrain and/or compel improved public-private partnership?
- How do relations between government and the private sector in potential adversary countries differ from those in the United States and its allies? What are the implications for cyber domain competition?

Silicon Valley and USG Relations:

Seligman, Lara. "Why the Military Must Learn to Love Silicon Valley." *Foreign Policy*, September 12, 2018. https://foreignpolicy.com/2018/09/12/why-the-military-must-learn-to-love-silicon-valley-pentagon-google-amazon/.

Seligman analyzes the future of Department of Defense (DoD) strategy, asserting that private sector collaboration is the course of action being taken by DoD for continued technological might. She points to military interest in utilizing advanced computing, big data analytics, artificial intelligence, and robotics as drivers of collaboration with the private sector. Seligman argues that DoD is aware that cooperation with Silicon Valley is essential, however, she asserts this is easier said than done. The bureaucratic practices and confidential nature of DoD projects clash loudly with the fast-pace, unbridled work essential to the success of Silicon Valley. With a rise in Chinese influence in the world of big tech, Seligman feels that the United States has no choice but to find a way to work with private companies to keep a competitive edge.

Zegart, Amy, and Kevin Childs. "The Divide Between Silicon Valley and Washington Is a National-Security Threat." *The Atlantic*, December 13, 2018. https://www.theatlantic.com/ideas/archive/2018/12/growing-gulf-between-silicon-valley-and-washington/577963/.

This article argues that a cultural rift exists between the tech industry and the Department of Defense which in turn impedes the ability for the two to cooperate and collaborate on national security issues. It explains that the rift between policymakers and technologists is based on conceptions of civil-military relations, knowledge regarding technology, and generational differences. The authors argue that closing this gap is a matter of national security and the best strategies for doing so include changing the messaging about government opportunities, building bridges between institutions, and overhauling the government's recruitment for these fields.

Cyber Vulnerabilities

The White House. *Vulnerabilities Equities Policy and Process for the United States Government.* 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

> In response to criticisms for a lack of transparency regarding its Vulnerabilities Equities Policy and Process (VEP), the White House published this unclassified version of the policy which outlines the process by which the government determines whether to disseminate or restrict information about newly discovered and not publicly known vulnerabilities in information systems and technologies. According to this document, the process generally follows the following steps: (1) submission to and notification of the VEP secretariat for a discovered vulnerability, (2) equity and discussions within the VEP secretariat, (3) decision to either disseminate or restrict disclosure, (4) follow-on actions regarding the decision (e.g., releasing vulnerability information to the vendor if decision to disseminate is reached).

Herr, Trey, Bruce Schneier, and Christopher Morris. "Taking Stock: Estimating Vulnerability Rediscovery." *Belfer Cyber Security Project White Paper Series*, 2017. https://www.belfercenter.org/sites/default/files/files/publication/Vulnerability%20Rediscovery.pdf.

> As opposed to the ample scholarly work focusing on the proportion of vulnerability discovery, Trey, Schneier, and Morris, tackle the issue of vulnerability rediscovery. Their work is an empirical analysis of vulnerability rediscovery in several types of software and across different vendors, studying the rate of discovery, the impact of time, the length of lag between original and duplicate discoveries, and the variation of all these factors across different vendors. Based on their findings, the authors note that rediscovery of vulnerability occurs more than twice as often as previously reported—although they believe that rediscovery rates are likely higher than what their research was able to conclude because they only looked at high to critical-severity vulnerabilities. Such results suggest that rediscovery of vulnerabilities kept secret by the NSA may be the source of up to one-third of all zero-day vulnerabilities detected in use each year. If this proves to be so, the authors recommend that the U.S. government rethinks its process for not disclosing software vulnerabilities.

Encryption and Backdoors:

Abelson, Harold, et al. "Keys under doormats: mandating insecurity by requiring government access to all data and communications." *Journal of Cybersecurity* 1, no. 1 (2015): 69-79. https://academic.oup.com/cybersecurity/article/1/1/69/2367066.

> As law enforcement organizations in the United States and the United Kingdom pushed for internet systems to be redesigned to ensure government access to information, this group of veteran computer scientists and security experts gathered to explore the implications of such proposals for "extraordinary access." The authors identified three general problems, including (1) the technical best practices for securing the internet would be compromised; (2) incorporating exceptional access would increase system complexity, greatly increasing security vulnerabilities; (3) exceptional access would be targeted by attackers. The article provides a historical context to exceptional access and gives an overview of law enforcement's current demands, specifically within the context of messaging services and through the use of personal electronic devices. The authors conclude that without a concrete technical proposal, legislators should reject any such proposals for extraordinary access to information.

Kuehn, Andreas, and Bruce McConnell. "Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions." EastWest Institute, 2018. https://www.eastwest.ngo/sites/default/files/ewi-encryption.pdf?dm_i=439P,3GU,17MEK,87B,1.

> This article seeks to explore the potential for encryption policy amongst democratic states. They analyze two encryption policy regime proposals, including (1) lawful hacking regimes and (2) design mandates, to enable legally authorized law enforcement access to encrypted data in specific situations. Lawful hacking would allow law enforcement to deploy lawful hacking as a technique to gain access to a system. Design mandates would rely on design mandates that require providers and manufacturers design, build, and deploy products and services that include the capability to accommodate future lawful access requests for information. The authors warn that these two policy regimes would have many associated risks but argue that greater cooperation across governments and companies is critical to protect privacy, fight crime and reduce compliance companies for all stakeholders involved.

Social Media Content Governance and Regulation

Stanford GDPi, Article 19, and David Kaye. *Social Media Councils: From Concept to Reality.* Conference Report, 2019. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/gdpiart_19_smc_conference_report_wip_2019-05-12_final_1.pdf.

> Building upon the premise that social media platforms, while beneficial for expressing opinions and sharing information, have also been used to incite violence, spread disinformation, and mobilize and recruit people to terrorist organizations, this report elaborates on the concept of Social Media Councils (SMC) as one method to deal with the

challenges posed by online content. The authors of this report maintain that government regulation of platforms can bring up serious free speech concerns and therefore suggest a multi-stakeholder approach of content moderation that can help avoid drawbacks stemming from both government and existing private sector approaches to content regulation. They expand upon the concept of SMCs by addressing key questions such as: whether the model should be industry-wide or platform-specific, whether SMCs should have advisory or adjudicatory authority, how should the interplay between national laws, international human rights law, and private sector terms of service and community guidelines be dealt with, and what type of structure would be most suitable for such SMCs.

Public-Private Relations in Russia and China

Bendett, Samuel, and Elsa B. Kania. "Chinese and Russian Defense Innovation, with American Characteristics? Military Innovation, Commercial Technologies, and Great Power Competition." *The Strategy Bridge*, August 2, 2018. https://thestrategybridge.org/the-bridge/2018/8/2/chinese-and-russian-defense-innovation-with-american-characteristics-military-innovation-commercial-technologies-and-great-power-competition.

Bendett and Kania examine government-initiated Chinese and Russian innovation communities focused on defense. It compares many of the initiatives and groups within these countries to similar efforts in the United States, including the Defense Advanced Research Projects Agency (DARPA), parallel innovation challenges, and industry partnerships. They conclude that while the United States still has a significant advantage in emerging technologies and their applications, Russian and Chinese efforts could nonetheless produce results that may yet disrupt today's techno-strategic competition among these great powers.

Suggested Further Reading:

1. Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford University Press, 2017.

2. Conti, Gregory, and David Raymond. *On Cyber: Towards an Operational Art for Cyber Conflict*. Kopidion Press, 2017.

3. DeNardis, Laura. *The Global War for Internet Governance*. Yale University Press, 2014.

4. Healey, Jason. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association, 2013.

5. Heather Harrison Dinniss. *Cyber Warfare and the Laws of War*. Cambridge University Press, 2012.

6. Kello, Lucas. *The Virtual Weapon and International Order*. Yale University Press, 2017.

7. Klimburg, Alexander. *The Darkening Web: The War for Cyberspace*. Penguin Press, 2017.

8. Lindsay, Jon, Tai Ming Cheung, and Derek Reveron, eds. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press, 2015.

9. Lin, Herbert, and Amy Zegart. *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Brookings Institution Press, 2019.

10. Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press, 2018.

11. Prunckun, Henry. *Cyber Weaponry*. Advanced Sciences and Technologies for Security Applications. Cham: Springer International Publishing, 2018.

12. Valeriano, Brandon, and Ryan C. Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press, 2015.

Center for Global Security Research
Lawrence Livermore National Laboratory
P.O. Box 808, L-189 Livermore, California 94551
https://CGSR.llnl.gov

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. LLNL-TR-779836